Simultaneous Measurements of the Channel Response for Multiple Eavesdroppers Operating in the Vicinity of a Body Area Network at 2.45 GHz

Bhargav, N., & Cotton, S. L. (2015). Simultaneous Measurements of the Channel Response for Multiple Eavesdroppers Operating in the Vicinity of a Body Area Network at 2.45 GHz. In *Proceedings of the 9th European Conference on Antennas and Propagation (EuCAP) 2015* Institute of Electrical and Electronics Engineers Inc.. http://www.eucap2015.org/files/EuCAP2015final_programme.pdf

Published in:
Proceedings of the 9th European Conference on Antennas and Propagation (EuCAP) 2015

Document Version:
Peer reviewed version

Queen's University Belfast - Research Portal:
Link to publication record in Queen's University Belfast Research Portal

Publisher rights
© 2015 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

General rights
Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The Research Portal is Queen's institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person's rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.

Download date:05. May. 2023

Queen's University Belfast

Queen's University Belfast - Research Portal

Simultaneous Measurements of the Channel Response for Multiple Eavesdroppers Operating in the Vicinity of a Body Area Network at 2.45 GHz

Bhargav, N., & Cotton, S. (2015). Simultaneous Measurements of the Channel Response for Multiple Eavesdroppers Operating in the Vicinity of a Body Area Network at 2.45 GHz. Paper presented at 9th European Conference on Antennas and Propagation (EuCAP), Lisbon, Portugal.

Document Version:
Author final version (often known as postprint)

Link:
Link to publication record in Queen's University Belfast Research Portal

Publisher rights
© 2015 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

General rights
Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The Research Portal is Queen's institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person's rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.

Download date:14. Jan. 2016

Simultaneous Measurements of the Channel Response for Multiple Eavesdroppers Operating in the Vicinity of a Body Area Network at 2.45 GHz

Nidhi Bhargav and Simon L. Cotton
Institute of Electronics, Communication & Information Technology
Queen's University Belfast, BT3 9DT, UK
{nbhargav01, simon.cotton}@qub.ac.uk

***Abstract*—Channel randomness can be exploited to generate secret keys. However, to ensure secrecy, it is necessary that the channel response of any eavesdropping party remain sufficiently de-correlated with that of the legitimate users'. In this paper, we investigate whether such de-correlation occurs for a body area network (BAN) operating in an indoor environment at 2.45 GHz. The hypothetical BAN configuration consisted of two legitimate transceivers, one situated on the user's left wrist and the other on the user's waist. The eavesdroppers were positioned in either a co-located or distributed manner in the area surrounding the BAN user. Using the simultaneous channel response measured at the legitimate BAN nodes and the eavesdropper positions for stationary and mobile scenarios, we analyze the *localized* correlation coefficient. This allows us to determine if it is possible to generate secret keys in the presence of multiple eavesdroppers in an indoor environment. Our experimental results show that although channel reciprocity was observed for both the stationary and the mobile scenarios, a higher de-correlation between the legitimate users' channels was observed for the stationary case. This indicates that mobile scenarios are better suited for secret key generation.**

***Index Terms*—secure communication, physical layer security, on-body measurements, correlation, fading characteristics, indoor communication.**

I. INTRODUCTION

Achieving a secrecy scheme that can be defended against potential eavesdroppers is important for the future security of body area networks (BANs). These networks have drawn a lot of attention for their use in healthcare applications. The limited power, memory, and the computational capabilities of BAN nodes, and the impact that could be caused by unauthorized access to sensitive information, presents significant challenges and motivation for implementing secure BAN communication.

Many key management protocols for wireless sensor networks have been proposed in [1, 2]. What is common amongst these studies is that they follow a conventional cryptographic approach to achieve secure communication. Recently, there has been a lot of research that follows information theoretic approaches for secret key generation. This involves exploiting properties of the physical layer; particularly, the random nature of the wireless channel to increase security. A theoretical foundation for this approach is given in [3]. Work proposed in [4-7], suggests that users sharing a common fading channel (as a result of the channel reciprocity property) can use the spatially dependent statistics of the channel to construct a shared secret key. Under the assumption that an eavesdropper's link is uncorrelated with the link between the legitimate parties, the eavesdropper is unable to establish this key. Thus, for the generation of secret keys, it is important that the two legitimate parties remain strongly correlated [8] and any eavesdropping channel remain sufficiently de–correlated with that of the legitimate parties; there by making it necessary to understand when such de-correlation occurs.

The measurement scenarios and techniques proposed here differ from that introduced in [9]. In the BAN context, the work in [9] assumed two eavesdroppers (Eves) with one positioned on the same body as the legitimate users (Alice and Bob) whilst the other was placed in an arbitrary position in the local surroundings. In this paper, however, we consider multiple co-located and distributed eavesdropping nodes positioned throughout the immediate environment with only the legitimate users positioned on the body. We therefore investigate whether the characteristics of the received signal for co-located and distributed eavesdropping positions are suitably uncorrelated with the signal characteristics at the legitimate parties to determine whether it is possible to achieve secure BAN communications in an indoor environment.

This paper is organized as follows. Section II describes the experimental setup and the measurement procedure. Section III contains a comparison of received signal power time series, and correlation coefficient between Alice, Bob and Eves for different scenarios considered for a BAN operating in an indoor environment. Lastly, Section IV concludes this paper and also suggests some future directions for the work.

II. EXPERIMENTAL SETUP AND MEASUREMENTS

The measurements conducted in this study were carried out in an open office area located on the first floor of the ECIT building at Queen's University Belfast in the United Kingdom. The building mainly consists of metal studded dry

This work was supported by the Department of Education and Learning (DEL) NI and in part by the U.K. Royal Academy of Engineering and the Engineering and Physical Research Council (EPSRC) under Grant Reference EP/H044191/1 and EP/L026074/1, and also by the Leverhulme Trust, UK.

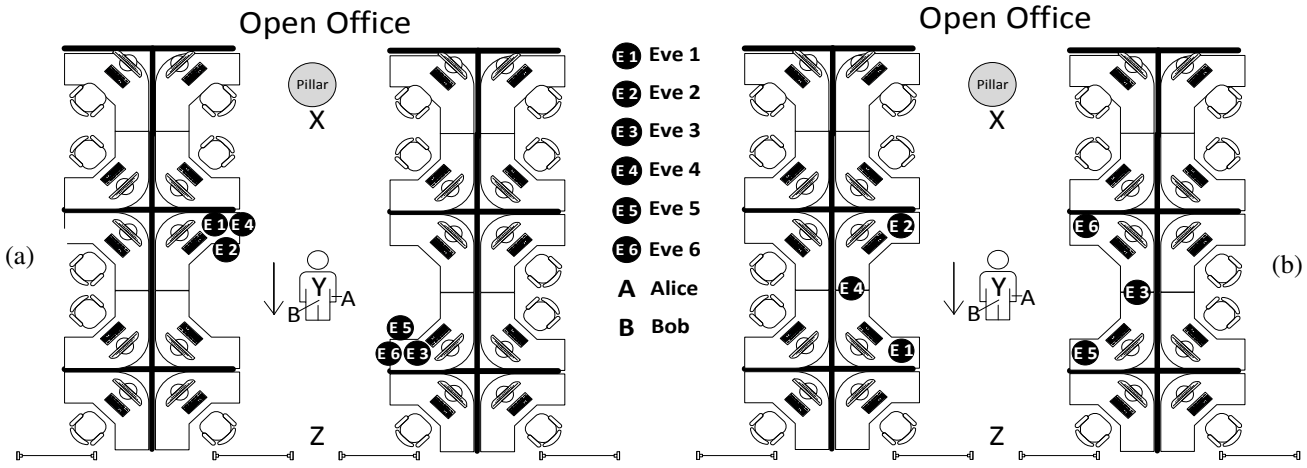

Fig.1 Open office area showing the position of Alice (node A), on the user's left wrist, Bob (node B), on the same user's waist, and Eves (node E's) for (a) co-located positioning of Eves and (b) distributed positioning of Eves. The test subject walked from point X to point Z and back for the mobile case and remained still at point Y for the stationary case.

walls with metal tiled floors covered with polypropylene-fiber, rubber backed carpet tiles, a metal ceiling with mineral fiber tiles and recessed louvered luminaries suspended 2.7 m above floor level. The office contained a number of chairs, metal storage spaces, doors and desks constructed from medium density fiberboard. These desks were separated by soft wooden partitions.

The test subject was an adult male of height 1.83 m and mass 80 kg. In the experiments conducted the antennas were mounted parallel to the body surface. The desired on-body link was established between two legitimate parties, Alice (node A), and Bob (node B). Alice was positioned on the left wrist of the test subject at a height of 1.15 m whilst Bob was positioned on the waist of the same test subject at a height of 0.98 m, and multiple eavesdroppers (Eves; node E's) were placed in fixed positions on surrounding desks. As illustrated in Fig. 1, two different eavesdropping configurations were considered. These were: (1) node E's are *co-located* i.e. side-by-side [Fig. 1(a)] and (2) node E's are distributed throughout the immediate environment [Fig. 1(b)].

Each of the A, B and E nodes consisted of an ML2730 transceiver, manufactured by RFMD. The transceiver boards were interfaced with a PIC32MX which acted as a baseband controller and allowed the analog received signal strength indicator (RSSI) to be sampled with a 10-bit quantization depth. For the channel measurements conducted here, Alice acted as the transmitter outputting a continuous wave signal with a power of +21 dBm.

Alice transmitted first by sending a trigger pulse to all the radio receivers. The receivers started the signal capture when it received the trigger signal. These measurements were then repeated with Bob acting as the transmitter and Alice being the receiver. All the other nodes were configured to record the RSSI simultaneously (i.e. time synchronized) with a sample frequency of 1 kHz. They utilized identical sleeve dipole antennas (Mobile Mark model PSKN3-24/555) which were vertically polarized throughout all of the experiments.

The experiments were performed in a choreographed manner when the office was unoccupied except for the test subject on which the legitimate nodes were placed. The test subject also moved in a repeatable manner for the experiments requiring motion. It should be noted that in order to enable as realistic a characterization of the signal correlation as possible, the wireless spectrum at the measurement frequency was uncontrolled, that is other wireless devices operating within the test environment may have acted as sources of interference.

In this study, we considered four distinct indoor scenarios. Our first and second experiment, herein referred to as *experiments 1* and *2,* respectively, were performed with the test subject remaining stationary at point Y with co-located node E's [Fig. 1(a)] and distributed node E's [Fig. 1(b)]. The third and fourth experiment, herein referred to as *experiments 3* and *4,* respectively, were carried out when the test subject walked from point X to point Z with co-located node E's [Fig. 1(a)] and distributed node E's [Fig. 1(b)].

III. Results and Analysis

A. Stationary Test Subject (Experiments 1 and 2)

These experiments were conducted to study the channel variations observed for a quasi-stationary scenario. The localized correlation coefficient between Alice-Bob, Alice-Eve and Bob-Eve channels were computed over a 0.5 second moving window over a 10 second period based on the Pearson product-moment correlation coefficient:

$$r = \frac{\sum_{i=1}^{n}(X_i - \overline{X})(Y_i - \overline{Y})}{\sqrt{\sum_{i=1}^{n}(X_i - \overline{X})^2}\sqrt{\sum_{i=1}^{n}(Y_i - \overline{Y})^2}} \qquad (1)$$

where, X_i and Y_i are the RSSI values of the ith packet of each node. $\overline{X}$ and $\overline{Y}$ are the respective mean RSSI values of a

sequence of n packets. Also, it should be noted that the correlation coefficient was calculated using the linear amplitude of the signal.

Table I shows the statistics of the correlation for experiments 1 and 2. As we can see, the mean correlation coefficients obtained here between the Alice-Bob, Alice-Eve and Bob-Eve channels were generally quite low. It is important to note that channel reciprocity was observed between the legitimate users'. However, in the stationary scenario as the mean signal level remains relatively constant, the observed low correlation between the legitimate nodes mainly occurred due to slight variations in the received signal caused by noise in the receiver. Because independent noise is observed at each of the users, a low correlation is seen.

For experiment 1 (co-located Eve nodes), the highest observed correlation coefficient was found to be 0.46, for the Bob-Eve6 link whereas for experiment 2 (distributed Eves), the highest observed correlation coefficient was found to be 0.78 for the Bob-Eve1 link. Both these exceed the correlation coefficient value obtained for the legitimate users. Therefore, the results show that a stationary environment is not suitable for key generation in an indoor BAN.

B. Co-located and Distributed Eavesdropper - Test Subject Walking (Experiment 3 and 4)

The variation in the received signal power measured by Alice, Bob and all of the Eves for experiments 3 and 4 are shown in Figs. 2 and 3 respectively. For the walking scenarios considered here, the channel displays some variation, with fluctuations between −28 dBm to −75 dBm. In BAN communications, it is anticipated that the movement of the human body may help to de-correlate the link with eavesdropping nodes, which are positioned in the local environment, with the legitimate on-body link. Figs. 4(a) and (b) show the normal probability density function (PDF) fitted to the empirical probability density of the localized correlation coefficient between Alice-Bob, Alice-Eve 4 and Bob-Eve 4, respectively. As we can see, the normal PDF provides a good fit to the empirical data (the mean and standard deviations are given in Table I).

It can also be seen from Figs. 4(a) and (b) that while the mean correlation coefficient is typically low, localized correlations greater than 0.70 can occur. In fact the largest correlation coefficient was found to be 0.81, which occurred for experiment 3 (co-located Eves), for the Alice-Eve4 channel. For the same experiment, the highest correlation coefficient value observed for the legitimate users' is 0.75. This indicates that for a co-located mobile scenario, generation of secret keys may not be possible. However, for experiment 4 (distributed Eves), the highest observed correlation coefficient was 0.80.This was greater than all the Alice-Eve and Bob- Eve channels. Based on these results, we can conclude that distributed mobile scenarios are better suited for key generation and secure communications can be achieved for this type of indoor BAN communications at 2.45 GHz.

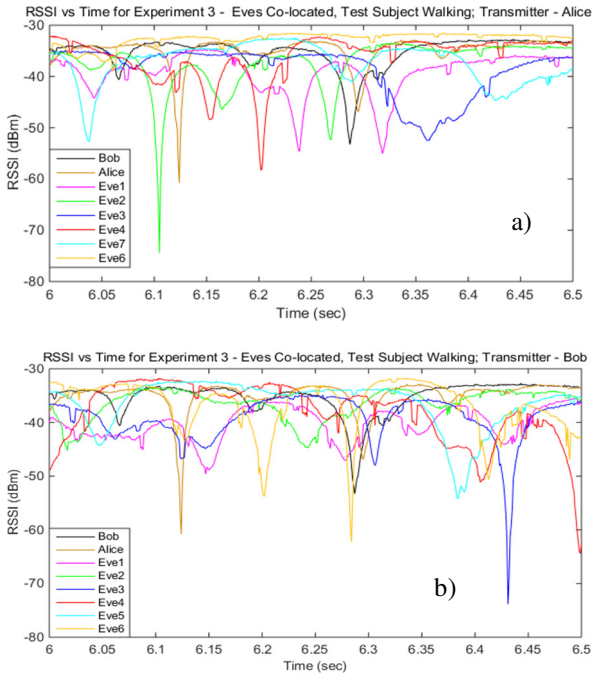

Fig. 2 RSSI (dBm) versus time (sec) for Experiment 3 - Eves co-located and test subject walking for a duration of 0.5 seconds with a) Alice as the transmitter and b) Bob as the transmitter.

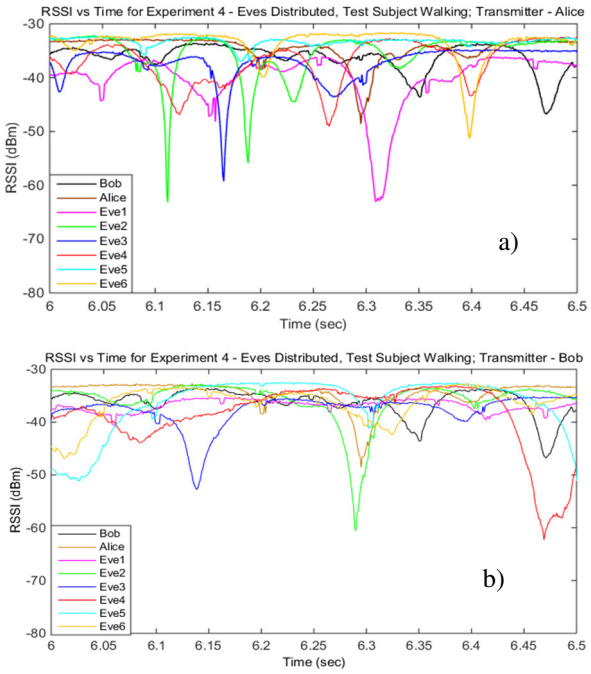

Fig. 3 RSSI (dBm) versus time (sec) for Experiment 4 - Eves distributed and test subject walking for a duration of 0.5 seconds with a) Alice as the transmitter and b) Bob as the transmitter.

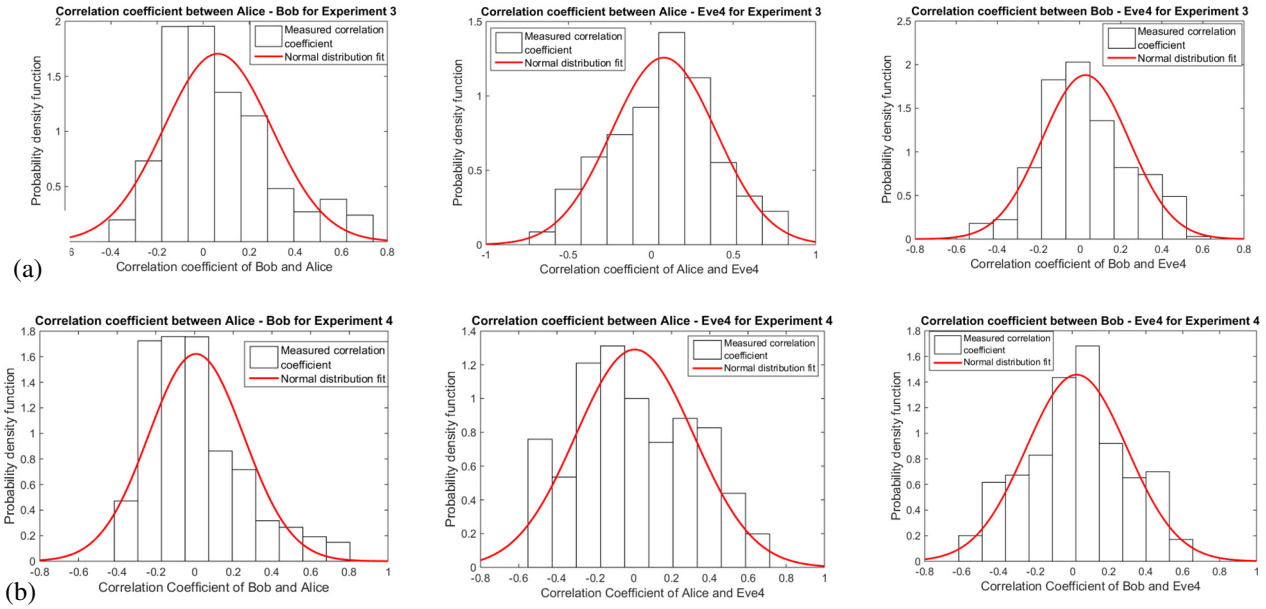

Fig.4 Correlation coefficient calculated between (a) Alice-Bob, Alice-Eve4 and Bob-Eve4 for Experiment 3 (test subject walking, Eves co-located) (b) Alice-Bob, Alice-Eve4 and Bob-Eve4 for Experiment 4 (test subject walking, Eves distributed). Also shown for comparison is the theoretical Gaussian probability density function which is shown to provide a good fit to the data.

TABLE I. MEAN AND STANDARD DEVIATIONS OF THE LOCALIZED CORRELATION COEFFICIENTS FOR EACH OF THE SCENARIOS

Eavesdroppers	Eve 1		Eve 2		Eve 3		Eve 4		Eve 5		Eve 6		
Legitimate Receivers	Alice	Bob	Alice	Bob	Alice	Bob	Alice	Bob	Alice	Bob	Alice	Bob	Alice-Bob
EXPERIMENT 1: STATIONARY TEST SUBJECT - EVES CO-LOCATED;													
Mean (μ)	0.01	0.05	0.09	0.05	0.08	0.13	0.01	0.01	0.12	0.27	0.01	0.04	0.02
Std. Deviation (σ)	0.05	0.08	0.08	0.12	0.06	0.08	0.05	0.10	0.05	0.09	0.03	0.10	0.04
EXPERIMENT 2: STATIONARY TEST SUBJECT - EVES DISTRIBUTED;													
Mean (μ)	0.07	0.20	0.05	0.01	0.06	-0.01	-0.06	-0.04	0.29	0.45	0.10	0.18	-0.08
Std. Deviation (σ)	0.09	0.33	0.14	0.34	0.11	0.30	0.15	0.11	0.16	0.11	0.15	0.29	0.13
EXPERIMENT 3: TEST SUBJECT WALKING - EVES CO-LOCATED;													
Mean (μ)	0.02	0.12	0.08	-0.03	0.02	0.51	0.08	0.03	-0.08	0.08	-0.09	0.01	0.06
Std. Deviation (σ)	0.28	0.22	0.23	0.23	0.25	0.27	0.32	0.21	0.24	0.21	0.25	0.29	0.23
EXPERIMENT 4: TEST SUBJECT WALKING - EVES DISTRIBUTED;													
Mean (μ)	-0.04	-0.18	0.02	-0.07	-0.02	-0.08	0.01	0.02	0.54	-0.00	-0.02	-0.01	0.01
Std. Deviation (σ)	0.21	0.20	0.29	0.22	0.24	0.29	0.31	0.27	0.26	0.26	0.29	0.31	0.25

IV. CONCLUSION AND FUTURE WORK

In this paper, we have measured the simultaneous channel response obtained for a desired on-body link and that obtained at multiple eavesdropper positions located in the immediate surroundings. Using this, we have investigated the localized correlation between the channel response at the legitimate and malicious users. The localized correlation coefficients suggest that secure key generation (and hence communication) can be achieved for this type of BAN communications in a mobile scenario. Future work will investigate the impact of the antenna type and polarization on secure BAN communications.

REFERENCES

[1] S. A. Çamtepe and B. Yener, "Key distribution mechanisms for wireless sensor networks: a survey," Computer Science Department, Rensselaer Polytechnic Institute, Troy, NY, USA, Technical Report TR-05-07, 2005.

[2] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," *Comput. Commun.*, vol. 30, no. 11–12, pp. 2314–2341, Sep. 2007.

[3] U. M. Maurer, “Secret key agreement by public discussion from common information,” *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733-742, 1993.

[4] R. Ahlswede and I. Csiszar, “Common randomness in information theory and cryptography. I. secret sharing,” *IEEE Transactions on Information Theory*, vol. 39. 1121-1132, Jul 1993.

[5] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, “Cryptographic key agreement for mobile radio,” *Digital Signal Processing*, vol. 6, no. 4, pp. 207-212, 1966.

[6] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, “Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel,” in *MobiCom'08*.

[7] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, “Robust key generation from signal envelopes in wireless networks,” in *CCS'07*.

[8] M. Wilhelm, I. Martinovic, and J. B. Schmitt, “Secure key generation in sensor networks based on frequency-selective channels,” *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1779-1790, September 2013.

[9] S. T. Ali, V. Sivaraman, and D. Ostry, “Secret key generation rate vs. reconciliation cost using wireless channel characteristics in body area networks,” *IEEE Trustcom*, 2010.